

**Европейская экономическая комиссия****Исполнительный комитет ЕЭК ООН****Центр Организации Объединенных Наций
по упрощению процедур торговли
и электронным деловым операциям**

Двадцать четвертая сессия

Женева, 30 апреля и 1 мая 2018 года

Пункт 7 b) предварительной повестки дня

**Рекомендации и стандарты: другие информационные
продукты для принятия к сведению****Белая книга о надежной трансграничной среде****Обеспечение юридически значимого надежного трансграничного
электронного взаимодействия***Резюме*

В процессе обмена информацией в электронной форме могут возникнуть вопросы по поводу юридической значимости соответствующих данных: иными словами, речь в этом случае идет о том, имеет ли полученная информация обязательную правовую силу. Данная Белая книга, в основу которой положена рекомендация 14 «Удостоверение подлинности внешнеторговых документов», содержит руководящие указания по поводу создания соответствующих условий взаимного признания в отношениях между странами в части юридической значимости информации в тех случаях, в которых требуются или желательны более высокие уровни достоверности. Такими условиями как раз и является надежная трансграничная среда. Эту работу можно было бы положить в основу соответствующей будущей работы по этой тематике.

Этот документ представляется участникам двадцать четвертой пленарной сессии для сведения.



I. Введение

1. Настоящий документ имеет целью облегчить и стимулировать создание надежной трансграничной среды для международного юридически значимого обмена электронными документами и данными между государственными органами и физическими и/или юридическими лицами. Данный документ предназначен для тех сторон, которые заинтересованы в создании, эксплуатации и практическом использовании таких трансграничных объектов инфраструктуры.

2. Сегодня Интернет стал обычным инструментом и той средой, которая позволяет отдельным лицам и субъектам из различных государств пользоваться соответствующими электронными услугами. Хотя преимущества таких услуг очевидны, тем не менее есть целый ряд организационных и правовых проблем, которые препятствуют их широкому использованию в тех случаях, когда сторонам требуется определенный уровень доверия в своих отношениях и в тех электронных услугах, которыми они пользуются. Один из основных вопросов состоит в том, чтобы обеспечить юридическую силу электронных документов и юридическую значимость электронного обмена данными в целом. Эта проблема носит срочный характер как на национальном (в рамках индивидуальных юрисдикций), так и на трансграничном уровне (когда возникают случаи взаимодействия между участниками, действующими в условиях юрисдикции различных государств).

3. Ниже показаны некоторые случаи, в которых требуется определенный *уровень доверия*:

- Электронные процедуры торгов, особенно в тех случаях, когда подрядчиком является соответствующий государственный орган или какая-либо крупная компания. Эти органы обычно нуждаются в высоком уровне надежности торговых документов их экономических операторов.
- Обмен некоторыми товарно-транспортными документами в рамках процедур трансграничной торговли.
- Процедуры разрешения споров и урегулирования исков, в том числе разрешение споров в онлайн-режиме. Эти процедуры предполагают необходимость однозначной идентификации и аутентификации истца и ответчика.
- Электронное страхование. В этом случае должен быть предусмотрен соответствующий механизм надежной проверки подлинности страхового свидетельства.

4. Проблема неотложности создания национальной среды безбумажной торговли находит отражение в некоторых региональных механизмах упрощения трансграничной торговли, например в Соглашении об упрощении процедур трансграничной безбумажной торговли в Азиатско-Тихоокеанском регионе, заключенном по линии Экономической и социальной комиссии ООН для Азии и Тихого Океана (ЭСКАТО). Одна из целей настоящей Белой книги состоит в оказании поддержки правительствам и региональным и международным организациям в создании таких сред и их управлении в условиях функциональной совместимости.

5. Как указано в рекомендации 14, СЕФАКТ ООН выступает за отказ от любых излишних правил, договоров или видов практики (там, где это возможно) в порядке упрощения процедур международной торговли. Тем не менее некоторые сценарии, связанные с торговлей, в случае которых участники стремятся обеспечить высокий *уровень доверия* в своих отношениях, продолжают сохраняться по сей день. Данная Белая книга как раз и посвящена урегулированию таких сценариев.

6. В указанной здесь Белой книге рассматриваются принципы создания и работы региональных и глобальных организаций по координации, которые обеспечивают условия доверия в сфере международного обмена данными и электронными документами между участниками, взаимодействующими в условиях электронной

среды (т. е. между государственными органами и физическими и юридическими лицами).

7. В ней затрагиваются в основном организационные и частично технические положения, регламентирующие услуги в области информационно-коммуникационных технологий (ИКТ). Положения, регламентирующие создание надлежащих правовых режимов, могут разрабатываться другими органами.

8. В общем и целом, данная Белая книга имеет целью оказать помощь в обеспечении защиты прав и законных интересов граждан и организаций в тех случаях, когда они производят *юридически значимые*¹ информационные операции в электронной форме с использованием Интернета и других общераспространенных систем ИКТ с открытым доступом.

9. Для того чтобы обеспечить более высокий *уровень доверия* к системе электронного взаимодействия, в Белой книге рассматривается вариант создания «общей инфраструктуры доверия» (ОИД) – фундаментальной, легко масштабируемой платформы, которая предусматривает специализированные пользующиеся доверием услуги ИКТ и обеспечивает унифицированный доступ к этим услугам.

10. СЕФАКТ ООН признает принцип технической нейтральности и не предлагает никакой иной специальной технологии в качестве основы ОИД. Право выбора технологий, которые обеспечат необходимый *уровень доверия* к процедуре электронного взаимодействия, принадлежит правительствам. В указанной Белой книге основное внимание обращается на организационные аспекты ОИД, а технические вопросы уточняются только в той степени, в которой это необходимо для изложения подходов, применимых на практике.

II. Базовый принцип общей инфраструктуры доверия

11. Участники процедуры электронного взаимодействия обычно занимаются какой-либо одной услугой ИКТ (электронная почта, облачное хранение данных, веб-порталы и т. п.). Если такие участники уже располагают достаточным *уровнем доверия* друг к другу и к услугам ИКТ, которыми они пользуются, то в этом случае ничего менять не требуется. Однако если участники не совсем уверены в своих отношениях и/или в услугах ИКТ, которыми они пользуются, то в этом случае, возможно, было бы целесообразно воспользоваться услугами третьей стороны, которая позволила бы повысить *уровень доверия* к процедуре электронного взаимодействия. Услуги, оказываемые этими доверенными третьими сторонами, получили название *удостоверительных услуг*.

12. В соответствии с данной Белой книгой *удостоверительные услуги* могут быть различных видов (выполнять различные функции) и обладать различными *уровнями спецификации*. *Удостоверительные услуги высокого уровня спецификации* оказываются на основании одного или нескольких международных соглашений и удовлетворяют установленным требованиям и соответствуют правилам, установленным соответствующими международными координаторами. *Удостоверительные услуги базового уровня спецификации* оказываются на основании одного или нескольких коммерческих соглашений и могут предусматриваться в рамках, например, крупномасштабных международных проектов и следовать признанным оптимальным видам практики, предусмотренным для провайдеров удостоверительных услуг. *Удостоверительные услуги* должны подвергаться аудиторской проверке в соответствии с их *уровнем спецификации*.

13. Совокупность *удостоверительных услуг*, используемых в соответствующих юридических, организационных и технических рамках, представляет собой *общую инфраструктуру доверия*. ОИД – это фундаментальная, легко масштабируемая

¹ Для придания процедуре электронного взаимодействия атрибута «юридической значимости» нужна соответствующая правовая основа, которая в данной Белой книге не рассматривается.

инфраструктурная платформа, обеспечивающая унифицированный доступ к *установленным услугам*.

14. Что касается электронного взаимодействия, то существующие естественные особенности различных регионов мира (исторические, культурные, политические, экономические, технические и т. п.) могут обусловить в пределах этих регионов различные *уровни доверия*.

15. Основная цель *ОИД* – обеспечить *юридически значимое* электронное взаимодействие между различными *уровнями спецификации* (нулевым, базовым, высоким) в части отношений между участниками процедуры электронного обмена.

16. Эта институциональная гарантия должна обеспечиваться в рамках деловых операций специализированных провайдеров, которые:

- оказывают пользователям *установленные услуги* в области ИКТ;
- действуют в условиях соблюдения установленных правовых режимов, которые включают ограничения, обусловленные обработкой личных данных, но не ограничиваются ими; и
- действуют в контексте общей инфраструктуры доверия.

III. Принципы создания *общей инфраструктуры доверия*

- **Масштабируемость.** ОИТ должна создаваться таким образом, чтобы ее можно было легко масштабировать. В этой связи необходимо предусмотреть возможность ее легкого масштабирования на любом уровне работы с учетом присоединения новых участников, таких как новые юрисдикции, новые наднациональные участники, новые провайдеры *установленных услуг* и новые системы регистрации.
- **Отслеживаемость.** Если это нужно участникам процесса электронного взаимодействия, то любой факт электронного взаимодействия на уровне ОИТ должен регистрироваться и, при необходимости, предъявляться для целей урегулирования конфликтов.
- **Затратоэффективность.** Принимая решение по тому или иному конкретному варианту архитектуры ОИД, необходимо учитывать результаты анализа риска. Расходы на создание и эксплуатации этой инфраструктуры должны быть меньше возможных убытков, вызванных сбоями в работе конкретных функций ИКТ и злонамеренными действиями.
- **Комплексность.** В процессе создания ОИД необходимо провести последовательную разработку правовых, организационных и технических вопросов. Комплексное описание позволит создать условия правильной работы всей системы в целом и каждого из ее элементов в отдельности.

IV. Согласованные подходы к *общей инфраструктуре доверия*

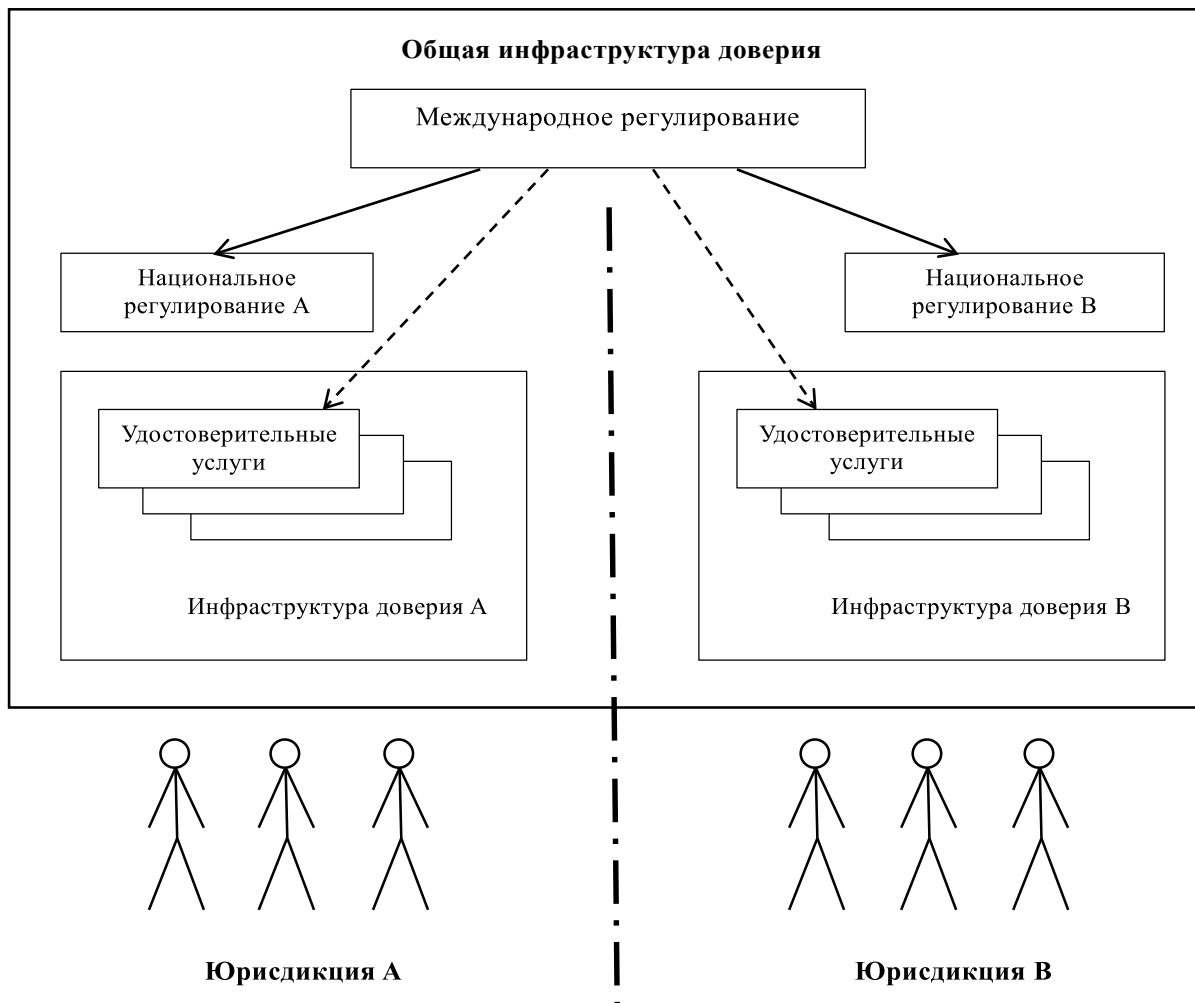
17. Выбор архитектуры *ОИД* производится в соответствии с принципами, изложенными в предыдущем разделе. Согласование осуществляется на трех уровнях *ОИД*: правовом, организационном и техническом.

A. Правовой уровень

18. *ОИД* можно построить на базе одного или нескольких *доменов*. В контексте правового и организационного регулирования самым сложным вариантом является база в составе нескольких *доменов*. На рис. 1 показана общая схема возможного подхода к правовому регулированию. Пунктирные стрелки указывают на те случаи, в

которых система национального регулирования отсутствует или в которых она практически невозможна.

Рис. 1
Правовой уровень



19. Правовое регулирование взаимодействия *ОИД* можно подразделить на два компонента: международный и национальный. Международное правовое регулирование осуществляется на основе следующих типов документов:

- международные договоры/соглашения;
- акты различных международных организаций;
- международные стандарты и правила;
- соглашения между участниками процесса трансграничного электронного взаимодействия по конкретным вопросам;
- типовые акты.

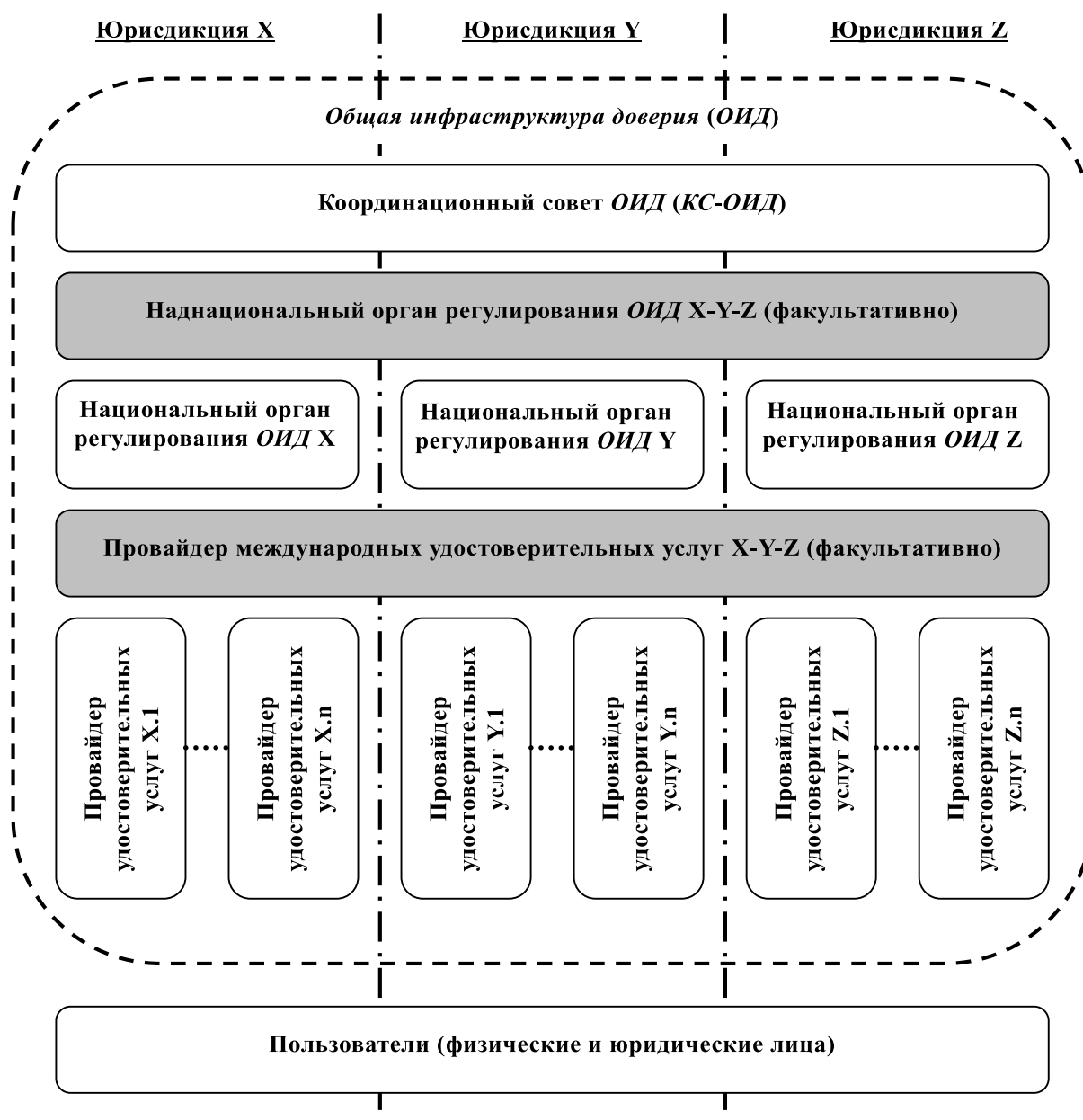
20. Национальное правовое регулирование строится на основе соответствующего свода нормативных документов, которые являются стандартными в каждой конкретной юрисдикции.

В. Организационный уровень

21. Взаимное *юридически значимое* признание электронных документов и данных, обработанных системой *удостоверительных услуг*, которые предоставляются в рамках

различных юрисдикций, можно обеспечить посредством создания и работы соответствующего специализированного органа (в этом примере он проходит под названием «Координационный совет *ОИД*» или *КС-ОИД*), который включает национальные органы регулирования, вошедшие в состав *КС-ОИД* по собственному желанию. Деятельность *КС-ОИД* может регулироваться соответствующим уставом *КС-ОИД*, который должен признаваться и подписываться всеми его уполномоченными членами, – т. е. органами регулирования электронного обмена данными в лице, прежде всего, национальных органов регулирования *ОИД*. На рис. 2 изображена общая схема координации на организационном уровне. Эти факультативные элементы в виде блоков выделены серым цветом.

Рис. 2

Организационный уровень

22. *КС-ОИД* издает ряд документов, взаимосвязанных с его Уставом:

- **Требования** к членам *КС-ОИД*: одним из необходимых предварительных условий получения статуса полноправного члена *КС-ОИД* является соблюдение установленных требований;

- **Руководящие принципы** осуществления «теневого» надзора за приемом в члены КС-ОИД и периодическая взаимная аудиторская проверка состояния членского состава в КС-ОИД;
- **Критерии соблюдения установленных требований**, которые должны соблюдаться провайдерами удостоверительных услуг, и методика применения этих критериев;
- **Схема оценки/проверки** провайдеров удостоверительных услуг в плане соблюдения ими этих критериев.

23. В *ОИД* каждая юрисдикция представлена национальным органом регулирования *ОИД* (см. рис. 2), который регулирует деятельность провайдеров *удостоверительных услуг* в своей юрисдикции.

24. В случае группы государств-членов с высоким уровнем интеграции (например, государств – членов Евразийского экономического союза или государств-членов Европейского союза) существует возможность учреждения наднационального органа регулирования *ОИД* (рис. 2: наднациональный орган регулирования *ОИД X-Y-Z*). В таком случае один наднациональный орган регулирования *ОИД X-Y-Z* заменяет собой группу национальных органов регулирования *ОИД X, Y и Z*.

25. Возможность естественной масштабируемости *ОИД* обеспечивается с помощью процедуры приема новых членов в состав *КС-ОИД* (новые национальные и наднациональные участники) и схемы проверки достоверности того факта, что провайдеры *удостоверительных услуг* удовлетворяют *критериям соблюдения требований*, издаваемым *КС-ОИД* (новые провайдеры *удостоверительных услуг*).

26. Международные провайдеры *удостоверительных услуг* могут установить нейтральные междоменные интерфейсы в качестве конкретного типа *удостоверительных услуг*. Основная функция междоменного интерфейса – обеспечить взаимное признание (легализацию) электронных документов и данных. Эти междоменные интерфейсы, соединяющие между собой отдельные *домены*, представляют собой элементы, на которых строится система *ОИД*.

27. Междоменные интерфейсы могут устанавливаться простым способом как на правовом и организационном уровнях, так и на комплексном уровне (правовом, организационном и техническом).

28. В первом случае сообщающиеся *домены* устанавливают общую правовую базу взаимного общения (см. «Правовой уровень» в разделе выше). Этот правовой уровень определяет весь спектр требований, условий и предпосылок, позволяющих и даже гарантирующих взаимное правовое признание (легализацию) *юридически значимых* электронных документов.

29. На организационном уровне процедуры и процессы взаимодействия между различными *доменами* подтверждают установленный *уровень доверия* между этими доменами в качестве достаточного для взаимного признания (легализации) электронных документов и данных, изданных в различных *доменах* или юрисдикциях.

30. В целях обеспечения этого необходимого *уровня доверия* данный свод требований, условий и предпосылок регулирует, в частности, создание и использование нейтральной международной среды, т. е. вне (за пределами) какого бы то ни было отдельного *домена*. Частью этой нейтральной международной среды являются *КС-ОИД* и провайдеры международных удостоверительных услуг. Такая нейтральная международная среда может использоваться в нейтральном правовом поле, которое определяется соответствующим международным органом.

31. В том случае, когда междоменные интерфейсы устанавливаются только на правовом и организационном уровнях, эти междоменные интерфейсы реализуются на практике только на основании соответствующих договоров, соглашений или организационных процедур. Эта правовая и организационная инфраструктура может поддерживаться различными *одиночными удостоверительными услугами*, такими как проверка электронной подписи, проверка полномочий, проставление временных

меток и т. п., но без указания конкретной *удостоверительной услуги*, имеющей целью выполнять функцию соответствующего интерфейса.

32. Во втором (комплексном) случае, когда междоменные интерфейсы создаются на правовом, организационном и техническом уровнях, такие интерфейсы дополнительно преобразуют соответствующий документ таким образом, чтобы он удовлетворял установленным требованиям (атрибуты, формат, структура и т. д.), которым должны удовлетворять *юридически значимые* электронные документы в *домене* получателя² (юрисдикции). Таким образом, *удостоверительная услуга* междоменного интерфейса может быть заменена целым рядом *удостоверительных услуг*, которые выполняют всего лишь отдельные конкретные функции (проверка электронной подписи, проверка полномочий, проставление временных меток и т. п.). Как всегда, *удостоверительные услуги* по линии междоменного интерфейса, реализованного на техническом уровне, будут и в этот случае предоставляться в соответствующей нейтральной международной среде.

33. Подходы к созданию междоменных интерфейсов должны учитывать использование переходных профилей, описывающих и конфигурирующих переходы из одного *домена* в другой. Эти переходные профили должны строиться с учетом, в частности, правовой основы взаимодействия между общающимися *доменами*, а также *уровней спецификации* соответствующих схем идентификации, используемых в пределах взаимодействующих *доменов*.

34. Для того чтобы получить статус национального провайдера *удостоверительных услуг*, поставщик этих услуг должен пройти аккредитацию у национального органа регулирования *ОИД* из той же юрисдикции. Провайдеры международных *удостоверительных услуг* должны пройти аккредитацию у *КС-ОИД*. Требования к аккредитации провайдеров *удостоверительных услуг* и требования к их деятельности должны регулироваться на основе критериев соответствия установленным требованиям, которые издаются *КС-ОИД*, и возможных национальных дополнений, издаваемых соответствующим национальным органом регулирования *ОИД*.

35. На уровне *КС-ОИД* пользователями электронных услуг могут быть как физические, так и юридические лица. Пользователи выбирают необходимый *уровень спецификации* соответствующей *удостоверительной услуги* по своему усмотрению или по договоренности.

36. Услуги должны оказываться соответствующими поставщиками – провайдерами *удостоверительных услуг*. Эти провайдеры *удостоверительных услуг* должны включаться по решению *КС-ОИД*.

37. *Удостоверительные услуги* в качестве элементов *ОИД* можно реализовать на практике самыми разными способами в зависимости от *уровня доверия* между *доменами* (юрисдикциями). Например, в случае условно «высокого» или «среднего» уровня взаимного доверия между членами *ОИД* одним из эффективных вариантов является система централизованных международных *удостоверительных услуг*, используемых в соответствии с согласованными нормами. В случае условно «низкого» *уровня доверия* система *удостоверительных услуг* строится на основе принципа децентрализации – национальная система *удостоверительных услуг* в каждой отдельной юрисдикции.

С. Технический уровень

38. На практике может быть множество технических вариантов реализации системы *удостоверительных услуг*. Основным требованием, предъявляемым к соответствующим компонентам *ОИД*, является функциональная совместимость. Правила на этом уровне применяются на основе различных стандартов и инструкций, закрепленных в соответствующих документах *КС-ОИД*.

² В случае отдельной юрисдикции «домен» или «удостоверительный домен» могут совпадать или могут объединять в своем составе несколько юрисдикций.

39. Для того чтобы обеспечить необходимую координацию на техническом уровне, в настоящей Белой книге рекомендуется организовать тесное сотрудничество с основными техническими организациями по стандартизации, таким как ИСО, ЕТСИ, W3C, ЕКС и другие³.

V. Удостоверительные инфраструктурные услуги: подходы к обеспечению технической совместимости

40. Для определения *удостоверительных услуг* целесообразно выяснить вопрос о том, нужны ли какие-либо атрибуты соответствующего базового документа для того, чтобы выполнить заложенную в него правовую функцию.

Таблица 1

Атрибуты документа, необходимые для выполнения его правовой функции

№	Тип атрибута	Обязательный да/нет	Описание/замечания
1.	Контент	да	<p><i>Контентом</i>, т. е. информационной сутью документа независимо от его формы (т. е. бумажной или электронной), является совокупность, включающая как минимум один из следующих атрибутов:</p> <ol style="list-style-type: none"> 1) тип документа; 2) классификация документа; 3) название документа; 4) содержание; 5) основная часть документа (обязательная); 6) приложения. <p>При этом в процессе обработки, хранения и передачи информации ее целостность и аутентичность не должны нарушаться.</p>
2.	Юридический статус издателя документа	да	<p><i>Юридическим статусом издателя документа</i> является совокупность следующих атрибутов:</p> <ol style="list-style-type: none"> 1) логотип; 2) название издателя; 3) справочные данные издателя (адрес, контакты и т. д.); 4) оттиск штампа.
3.	Статус (полномочия) подписавшей стороны или ее должность	нет	<p>Краткое описание полномочий подписавшей стороны с указанием их срока действия.</p>
4.	Подпись	да	<p><i>Подписью</i> является совокупность следующих атрибутов:</p>

³ Международная организация по стандартизации (ИСО), Европейский институт по стандартизации в области электросвязи (ЕТСИ), консорциум «Всемирная паутина» (W3C), Европейский комитет по стандартизации (ЕКС).

№	Тип атрибута	Обязательный да/нет	Описание/замечания
			1) подпись издателя; 2) штамп подтверждения с факсимиле; 3) штамп утверждения с факсимиле; 4) виза (штамп разрешения/одобрения); 5) штамп подтверждения подлинности копии; 6) печать организации, издавшей документ; 7) прочее.
5.	Время	да	Указание времени подписания на основе надежного источника времени (аспект действительности).
6.	Место	нет	Указание места подписания (место, в котором подписавшая сторона оформила свое волеизъявление путем проставления своей подписи) является факультативным. Если этот тип услуги недоступен, то одним из атрибутов <i>контента</i> можно считать атрибут <i>места</i> .

41. Базовые типы *удостоверительных услуг* (функции удостоверительных услуг, выполняемые по конкретному запросу):

- a. создание, проверка и подтверждение подлинности подписей и печатей;
- b. проверка юридического статуса;
- c. создание, проверка и подтверждение подлинности временных меток;
- d. обеспечение нейтральных междоменных интерфейсов;

Примечание: Если между доменами (юрисдикциями) установлен соответствующий интерфейс, то в этом случае необходимо предусмотреть соответствующий профиль этого междоменного интерфейса на основе соответствующего соглашения между этими доменами. Каждый междоменный интерфейс должен «знать» те атрибуты, которые являются обязательными для каждого домена. На техническом уровне междоменный интерфейс должен выполнять функцию протокольного перевода или перевода различных протоколов при переходе из одного домена в другой. Математическое описание функций междоменного интерфейса см. в приложении 2. Удостоверительные услуги (в том числе междоменные интерфейсы) предоставляются на основе национальных схем идентификации, с одной стороны, и на основе надежной международной инфраструктуры (других удостоверительных услуг) – с другой.

- e. обеспечение идентификации физических и юридических лиц.

42. Нижеследующие типы атрибутов (см. таблицу 1) предполагают необходимость предварительной идентификации соответствующих физических или юридических лиц:

- юридический статус издателя документа;
- статус (полномочия) подписавшей стороны или ее должность;
- подпись.

43. В случае *удостоверительных услуг* типа a) и b) используются эти типы атрибутов, которые, как следствие, предполагают также необходимость

предварительной идентификации соответствующих физических или юридических лиц. Услуги по идентификации предоставляются провайдерами, которые специализируются на выполнении процедуры идентификации. Эти услуги могут оказываться на различных *уровнях спецификации*: нулевом, базовом и высоком. КС-ОИД утверждает/согласует подходящие схемы идентификации и/или ссылки на доведенные до его сведения схемы идентификации в пределах отдельного домена.

44. Некоторые атрибуты идентификации и сами процедуры идентификации могут служить основой для определения соответствующих *уровней спецификации* схем идентификации. *Уровни спецификации* различных схем идентификации могут представлять собой важнейший элемент регулирования взаимодействия между различными доменами. Соответствующие совокупности атрибутов могут определяться правовыми режимами коммерческой деятельности провайдеров, которые специализируются на выполнении процедуры идентификации, и провайдеров функциональных услуг. Соответствующие совокупности атрибутов могут поддерживаться на уровне системы *удостоверительных услуг* (услуги по идентификации). Деятельность провайдеров, которые специализируются на выполнении процедуры идентификации, может регулироваться в соответствии с особыми организационными и техническими требованиями, разработанными в целях обеспечения защиты личных данных.

45. Примечание: долговременную систему услуг по архивированию и связанной с этим проверке можно реализовать на практике в качестве соответствующей функции услуги ИКТ или функции доверительной услуги особого типа.

46. Примечание: В целях сведения до минимума соответствующих требований, касающихся обновления существующих электронных систем и их соединения с ОИД, этот момент необходимо должным образом принимать во внимание.

VI. Уровни спецификации услуг общей инфраструктуры доверия

47. *Уровень спецификации удостоверяющих услуг* представляет собой одну из функций удостоверяющих услуг, позволяющих очевидным образом удовлетворить заранее определенный комплекс требований.

48. *Уровни спецификации* той или иной *удостоверительной услуги* могут носить нарастающий характер. Чем ниже степень доверия участников друг к другу и к услугам ИКТ по обработке электронных операций в части взаимодействия (т. е. создание, доступ, преобразование, передача, уничтожение и т. п.), тем жестче требования к *уровню спецификации* соответствующих *удостоверительных услуг*.

49. Параметры *уровней спецификации удостоверяющих услуг* описаны в нижеследующей таблице.

Таблица 2

Параметры уровней спецификации удостоверяющих услуг

	Степень доверия участников друг к другу и к услугам ИКТ		
	Высокая степень доверия	Существенная степень доверия	Ограниченная степень доверия
Уровни спецификации удостоверяющих услуг	Удостоверительные услуги не нужны («нулевой» уровень спецификации)	Базовый уровень спецификации	Высокий уровень спецификации

	Степень доверия участников друг к другу и к услугам ИКТ		
	Высокая степень доверия	Существенная степень доверия	Ограниченная степень доверия
Правовой режим операции по удостоверительным услугам	н/п	На основе коммерческих соглашений и/или общепринятой торговой практики	На основе международных соглашений (конвенций) и/или непосредственно применимых международных правил ⁴
Организационная инфраструктура удостоверительных услуг	н/п	Любые крупномасштабные проекты	Координационный совет по ОИД (КС-ОИД), см. раздел IV выше
Технические требования к удостоверительным услугам	н/п	Соответствие провайдеров удостоверительных услуг требованиям признанной оптимальной практики	– Удовлетворение критериев соответствия КС-ОИД и – Удовлетворение требованиям, изложенным в применимых национальных правилах (для национальных провайдеров удостоверительных услуг)

50. Если *удостоверительные услуги*, задействованные в течение жизненного цикла данного документа (включая систему междоменных интерфейсов, действующих между издателем документа и его получателем), характеризуются различными *уровнями спецификации*, то общий уровень спецификации будет равен самому низкому из них.

VII. Взаимодействие с организациями в различных областях стандартизации

51. В настоящей Белой книге предлагается разработать описание различных возможных правовых режимов:

- на основе международных соглашений (конвенций) и/или непосредственно применимых международных правил;
- на основе коммерческих соглашений и/или общепринятой торговой практики;
- без особых международных правил.

52. Правовые режимы могут дополнительно поддерживаться традиционными учреждениями (государственными органами, судебными постановлениями, системой страхования рисков, государственными нотариусами и другими субъектами) посредством взаимного признания электронных документов, подтвержденных на уровне системы *удостоверительных услуг*.

53. Сложившиеся правовые режимы могут также использоваться для распространения особых требований на материалы и финансовую поддержку коммерческой деятельности специализированных провайдеров в случае причинения ущерба их пользователям, в том числе в случае нарушения целостности данных.

⁴ Например, *удостоверительные услуги*, оказываемые в соответствии с Регламентом ЕС (eIDAS) или соглашением Евразийского экономического союза и иными документами.

54. Институциональные гарантии и правовые режимы, позволяющие формировать и обеспечивать работу региональных и глобальных надежных трансграничных условий, должны рассматриваться в отдельном документе соответствующим специализированным органом.

55. В данном документе предлагается описание механизмов взаимодействия между отдельными государствами и их международными союзами, использующими иные международные форматы, в целях создания общей надежной трансграничной среды.

- a. Посредством полного или частичного присоединения того или иного государства к существующему правовому режиму на основе международных договоров и/или посредством прямого применения международных норм, в контексте которых задача по формированию региональной надежной трансграничной среды уже была поставлена или решена. Этот существующий правовой режим обеспечивает субъектам электронного взаимодействия соответствующие институциональные гарантии.
- b. В контексте взаимодействия между различными международными союзами:
 - на первом этапе группа государств создает соответствующий региональный домен, обеспечивающий субъектам электронного взаимодействия соответствующие институциональные гарантии в рамках соответствующего правового режима, установленного этими государствами;
 - на втором этапе уточняются протоколы доверительного взаимодействия с другими международными союзами в части взаимного признания различных правовых режимов. Это взаимное признание распространяется на институциональные гарантии и требования к информационной безопасности каждого из международных форматов, по возможности, на базе соответствующего междоменного интерфейса, действующего в рамках данного международного правового режима.
- c. В контексте взаимодействия одного государства с другими государствами или с международными союзами:
 - на первом этапе государство создает свой собственный домен, действующий в рамках соответствующего правового режима, установленного этим государством;
 - на втором этапе уточняются протоколы доверительного взаимодействия с другими государствами и/или международными союзами в части взаимного признания различных правовых режимов. Такое взаимное признание строится с учетом институциональных гарантий и требований к информационной безопасности, предусмотренных этими государствами и международными форматами, по возможности, на базе соответствующего междоменного интерфейса, действующего в рамках данного международного правового режима.

VIII. Связи с международными организациями в различных областях стандартизации по вопросам формирования действующей надежной трансграничной среды

56. В настоящей белой книге предлагается принимать во внимание следующие аспекты стандартизации:

Технические аспекты

57. Основная цель стандартизации в этой области состоит в содействии разработке стандартов технической совместимости в пределах данной надежной трансграничной среды. Эта работа должна охватывать все технические аспекты, которые в любом случае воздействуют на функциональную совместимость и безопасность, например на документы и форматы данных, протоколы связи, форматы и протоколы конверсии, технические интерфейсы, обеспечение равнозначного уровня качества (безопасности) технических компонентов и т. д.

Организационные аспекты

58. Основная цель стандартизации в этой области состоит в поддержании соответствующего *уровня доверия* между доменами, который был бы достаточным для взаимного признания (легализации) электронных документов и данных, которые издаются в различных *доменах* (юрисдикциях). Это, в частности, включает процедуры осуществления аудиторской проверки провайдеров *удостоверительных услуг* независимыми органами, которые проводят оценку соответствия установленным требованиям; аккредитации этих органов по оценке соответствия; взаимной аудиторской проверки на коллегиальной основе между членами Координационного совета *ОИД*, объектами и областями, подлежащими аудиту, и применимыми критериями аудиторской проверки.

59. В этой работе следует учитывать конкретные аспекты, поскольку они применимы к различным *уровням спецификации удостоверительных услуг*. Если та или иная *удостоверительная услуга* с более низким *уровнем спецификации* взаимодействует с *удостоверительной услугой* с более высоким *уровнем спецификации*, то уровень спецификации всей цепочки взаимодействия *удостоверительных услуг* будет, в лучшем случае, равным более низкому *уровню спецификации*.

Приложение I

Глоссарий

Курсив указывает на те термины, которые определены для целей настоящей Белой книги.

Для целей настоящего документа используются следующие термины:

- **Общая инфраструктура доверия (ОИД)**
 - Инфраструктура, предназначенная для целей содействия обеспечению *юридической значимости* трансграничного электронного взаимодействия. *ОИД* предоставляет соответствующий комплекс *удостоверительных услуг*, согласованных на правовом, организационном и техническом уровнях.
- **Степень доверия** (участников системы электронного обмена друг к другу и к услугам ИКТ по обработке операций в части электронного взаимодействия между ними)
 - Общественно необходимая функция установленного или осязаемого доверия участников системы электронного обмена друг к другу и к услугам ИКТ по обработке операций в части электронного взаимодействия между ними.
- **Юридическая значимость** (соответствующего действия)
 - Свойство соответствующего действия (процесса), которое(ый) позволяет инициировать создание (или сводиться к созданию) документов (единиц данных), обладающих *юридической действительностью*.
- **Юридическая значимость** (документа)
 - Свойство документа (единицы данных), позволяющее изменить правовой статус соответствующего субъекта права (физического или юридического лица, которое по праву обладает способностью осуществлять права и юридические обязанности).
 - *Юридически значимый* документ всегда является также *юридически действительным* документом с конкретным содержанием.
- **Юридическая действительность** (также называемая «*юридической силой*») (документа)
 - Свойство документа (единицы данных), подлежащее применению для целей судопроизводства, т. е. рассматриваемое как удовлетворяющее требованиям применимого права. *Юридическая действительность* придается тому или иному документу на основании действующего законодательства органом, который его издал, и в соответствии с действующим порядком его издания (например, его можно использовать в качестве реферативного материала).
- **Уровень спецификации** (или спецификационный уровень) (услуги)
 - Свойство услуги, позволяющее очевидным образом выполнить предварительно установленную совокупность требований.
- **Уровни доверия** (между областями)
 - Общественно необходимая функция, позволяющая определить степень доверия между *доменами*.
 - В зависимости от установленного *уровня доверия домены* готовы для обмена некоторым объемом ресурсов и совместного использования некоторых объектов инфраструктуры; иными словами, *домены* готовы для передачи части присущих им полномочий, функций и ресурсов в

пользование *общей инфраструктуре доверия (ОИД)*, которой они доверяют на совместной основе. Чем выше *уровень доверия* к этой *ОИД*, тем больше полномочий, присущих *доменам*, они готовы передать *ОИД*.

- **Домен** (домен доверительных отношений)
 - Информационное и правовое пространство, используемое одной и той же *ОИД*. *Домен* может совпадать с какой-либо одной юрисдикцией или объединять в своем составе несколько юрисдикций.
- **Удостоверительная услуга**
 - (определение высокого уровня) – электронная служба, имеющая целью обеспечить некоторую *степень доверия* между участниками процесса электронного взаимодействия.
- **Доверительное электронное взаимодействие**
 - Обмен любыми данными в электронной форме таким образом, что пользователь этих данных однозначно принимает их как достоверные в соответствии с действующими принципами работы. Принципы работы каждого пользователя позволяют установить, можно ли считать данную операцию электронного взаимодействия достоверной. Как следствие, достоверность данных, полученных в результате электронного обмена, варьируется в зависимости от пользователя. В ходе любого процесса электронного взаимодействия используются системы услуг информационно-коммуникационной технологии (такие, как система интернет-услуг, система услуг электронной почты, любые службы обмена сообщениями, система облачного хранения данных и т. п.); вместе с тем *доверительное электронное взаимодействие* обеспечивается посредством использования *удостоверительных услуг*.

Приложение II

Математическое описание функций междоменного интерфейса

Для работы междоменного интерфейса необходимо разработать соответствующий комплекс правил, позволяющих производить конверсию соответствующих требований между двумя доменами А и В.

$$A=\{a_1, a_2, \dots, a_N\}$$

$$B=\{b_1, b_2, \dots, b_M\}$$

$$E(a)=A \rightarrow B,$$

где А – комплекс требований (атрибутов) для домена А, В – комплекс требований для домена В и E(a) – комплекс правил преобразования данных, поступающих из А в В. С учетом того, что объем этих комплексов (т. е. количество требований) в реальных условиях не может быть равным ($N \neq M$), необходимо разработать правила, позволяющие привести оба эти комплекса к одинаковому знаменателю К, где $K=\text{MAX}(N, M)$.

Степень доверия к этому комплексу правил преобразования можно определить как возможность преобразования этих комплексов в некоторый универсальный суперкомплекс требований с учетом того, что это преобразование производится внутри каждого домена.

$$E(a)=A \rightarrow X$$

$$E(x)=X \rightarrow B,$$

где X – универсальный суперкомплекс требований к А и В.